UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,904	05/01/2001	Soon-Young Cho	KPLO 7025	4645

321 7590 12/21/2004

SENNIGER POWERS LEAVITT AND ROEDEL
ONE METROPOLITAN SQUARE
16TH FLOOR
ST LOUIS, MO 63102

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,904	CHO ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-59 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-59 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-59 have been examined and is rejected *under 35 U.S.C. 103(a)*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wailewski, et al. (US 6,424,714), and further in view of Kupka, et al. (US 6,434,535).

As per claim 1

Wailewski, et al. discloses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods, comprising:

a digital goods section including digital goods to be sold via online from a business proprietor to a client; **[COL.1, lines 50-57]**

a physical goods to be operated by contents of the digital goods **[COL.5, lines 44-49]**, the physical goods having an inherent ID given thereto **[COL.2, lines 35-39]**, a first encrypted ID also given thereto and encrypted according to

a first encryption algorithm from said inherent ID **[COL.3, lines 64-66]**, and an assignable identification name for identifying the physical goods; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

a controller for examining whether or not the client is a genuine proprietor of the physical goods based on information including the assignable identification name and the inherent ID of the physical goods **[COL.7, lines 47-52 and COL.21, lines 18-34]**, generating a second encrypted ID by encrypting the first encrypted ID of the physical goods according to a second encryption algorithm **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, encrypting the digital goods for which the client has made a request for purchase according to the second encryption algorithm **[COL.4, lines 3-5 and COL.7, lines 44-45]**, and transferring the second encrypted ID and the encrypted digital goods to the client, when selling the digital goods; and **[COL.4, lines 6-8]**

making the request for purchase of the digital goods based on the assignable identification name and a selection of digital goods desired for purchase **[COL.7, lines 15-37]**, and transferring the encrypted digital goods and the second encrypted ID to the physical goods when the second encrypted ID and the encrypted digital goods are transferred to the client interface section from the controller **[COL.22, lines 56-64]**, wherein the physical goods decrypts the second encrypted ID transferred from the client interface section according to a decryption algorithm, thereby extracting the first encrypted ID **[COL.11,**

lines 43-57 and COL.23, lines 13-23], and if the extracted first-encrypted ID coincides with the first encrypted ID given to the physical goods **[COL.6, lines 32-40]**, decrypts the encrypted digital goods transferred from the client interface section according to the decryption algorithm and executes the decrypted digital goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process to show a genuine proprietor of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Wasilewski with the teachings of Kupka to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 2

Wailewski discloses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods, comprising:

a digital goods section including digital goods to be sold via online from a business proprietor to a client a physical goods to be operated by contents of

the digital goods **[COL.1, lines 50-57 and COL.5, lines 44-49]**, the physical goods having an inherent ID given thereto, a first encrypted ID also given thereto and encrypted according to a first encryption algorithm from said inherent ID, and an assignable identification name for identifying the physical goods; **[COL.2, lines 35-48 and COL.3, lines 64-66]**

a controller for examining whether or not the client is a genuine proprietor of the physical goods based on information including the assignable identification name and the inherent ID of the physical goods **[COL.7, lines 47-52 and COL.21, lines 18-34]**, generating a second encrypted ID by encrypting the first encrypted ID of the physical goods according to a second encryption algorithm **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, encrypting the digital goods for which the client has made a request for purchase according to the second encryption algorithm **[COL.4, lines 3-5 and COL.7, lines 44-45]**, and transferring the second encrypted ID and the encrypted digital goods to the client, when selling the digital goods; and **[COL.4, lines 6-8]**

making the request for purchase of the digital goods based on the assignable identification name and a selection of digital goods desired for purchase **[COL.7, lines 15-37]**, and transferring the encrypted digital goods and the second encrypted ID to the physical goods when the second encrypted ID and the encrypted digital goods are transferred to the client interface section from the controller **[COL.22, lines 56-64]**, wherein the physical goods decrypts

the second encrypted ID and the encrypted digital goods transferred from the client interface section according to a decryption algorithm **[COL.11, lines 43-57 and COL.23, lines 13-23]**, thereby extracting the first encrypted ID and digital contents, and if the extracted first-encrypted ID coincides with the first encrypted ID given to the physical goods, executes the contents of the decrypted digital goods **[COL.10, lines 43-55 and col.23, lines 30-39]** . **Wasalewski fails to explicitly discuss the registering process to show a genuine proprietor of the physical goods.**

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 3

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 1, wherein both the inherent ID and the first encrypted ID are incorporated into the physical goods

during manufacture of the physical goods. **[COL.10, lines 27-28]**

As per claim 4

Wailewski dicusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 1, wherein the first encrypted ID given to the physical goods can be inputted from outside of the physical goods after manufacture of the physical goods. **[COL.10, lines 32-38] [COL.10, lines 27-28]**

As per claim 5

Wailewski discloses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods, comprising:

a digital goods section including digital goods, said digital goods including a first operation portion and a second operation portion and saleable via online from a business proprietor to a client; **[COL.1, lines 50-57 and COL.5, lines 44-49]**

a physical goods to be operated by contents of the second operation portion of the digital goods, the physical goods having an inherent ID given thereto **[COL.3, lines 64-66]**, a first encrypted ID also given thereto and encrypted according to a first encryption algorithm from said inherent ID and an assignable identification name for identifying the physical goods; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

a controller for examining whether or not the client is a genuine proprietor of the physical goods based on information including the assignable

identification name and the inherent ID of the physical goods **[COL.7, lines 47-52 and COL.21, lines 18-34]**, generating a second encrypted ID by encrypting the first encrypted ID of the physical goods according to a second encryption algorithm **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, encrypting the digital goods for which the client has made a request for purchase according to the second encryption algorithm **[COL.4, lines 3-5 and COL.7, lines 44-45]**, and transferring the second encrypted ID and the encrypted digital goods to the client, when selling the digital goods; and **[COL.4, lines 6-8]**

making the request for purchase of the digital goods based on the assignable identification name and a selection of digital goods desired for purchase **[COL.7, lines 15-37]**, separating the digital goods into a first execution portion and a second execution portion if the second encrypted ID and the digital goods requested for purchasing are transferred from the controller **[COL.10, lines 1-8]**, and transferring the separated second execution portion and the second encrypted ID to the physical goods **[COL.4, lines 20-30]**, wherein the physical goods decrypts the second encrypted ID transferred from the client interface section according to a decryption algorithm **[COL.11, lines 43-57 and COL.23, lines 13-23]**, thereby extracting the first encrypted ID, and if the extracted first-encrypted ID coincides with the first encrypted ID given to the physical goods **[COL.6, lines 32-40]**, executes contents of the second execution portion transferred from the client interface

section, and wherein when the contents of the second execution portion of the digital goods are executed in the physical goods, the client interface section executes the first execution portion of the digital goods in synchronization with the execution of the contents of the second execution portion **[COL.9, lines 32-36]. Wasalewski fails to explicitly discuss the registering process to show a genuine proprietor of the physical goods.**

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 6

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 5, wherein both the inherent ID and the first encrypted ID are incorporated into the physical goods during manufacture of the physical goods. **[COL.10, lines 27-28]**

As per claim 7

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 5, wherein the first encrypted ID given to the physical goods can be inputted from outside of the physical goods after manufacture of the physical goods. **[COL.10, lines 32-38]**

As per claim 8

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 5, wherein the physical goods prohibits the execution of the first execution portion of the digital goods in the client interface section if the extracted first-encrypted ID does not coincide with the first encrypted ID given to the physical goods. **[COL.6, lines 6-22 and COL.11, lines 46-59]**

As per claim 9

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 5, wherein the physical goods is a storytelling device, and the second execution portion includes operation code for controlling operation of the physical goods according to contents of a story and narration for dictating the contents of the story. **[COL.5, lines 44-55]**

As per claim 10

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 5, wherein the

controller simultaneously transfers to the client the second encrypted ID and the digital goods requested by the client for purchase. **[COL.4, lines 1-19]**

As per claim 11

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 9, wherein the client interface is a personal computer, and the first execution portion of the digital goods includes images and sound effects. **[COL.5, lines 44-55]**

As per claim 12

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods, comprising:

a digital goods section including digital goods, said digital goods including a first operation portion and a second operation portion and saleable via online from a business proprietor to a client; **[COL.1, lines 50-57 and COL.5, lines 44-49]**

a physical goods to be operated by contents of the second operation portion of the digital goods, the physical goods having an inherent ID given thereto, a first encrypted ID also given thereto and encrypted according to a first encryption algorithm from said inherent ID, and an assignable identification name for identifying the physical goods; **[COL.2, lines 35-48 and COL.3, lines 64-66]**

a controller for examining whether or not the client is a genuine proprietor of the physical goods based on information including the assignable

identification name and the inherent ID of the physical goods **[COL.2, lines 44-48 and COL.6, lines 37-40]**, generating a second encrypted ID by encrypting the first encrypted ID of the physical goods according to a second encryption algorithm, encrypting the digital goods for which the client has made a request for purchase according to the second encryption algorithm **[COL.4, lines 3-5 and COL.7, lines 44-45]**, and transferring the second encrypted ID and the encrypted digital goods to the client, when selling the digital goods; and

making the request for purchase of the digital goods based on the assignable identification name and a selection of digital goods desired for purchase **[COL.7, lines 15-37]**, separating the digital goods into a first execution portion and a second execution portion if the second encrypted ID and the digital goods requested for purchasing are transferred from the controller **[COL.10, lines 1-8]**, transferring the second encrypted ID to the physical goods, and transferring the second execution portion of the digital goods to the physical goods according to the request for transfer of the second execution portion of the digital goods made by the physical goods **[COL.4, lines 20-30]**, wherein the physical goods decrypts the second encrypted ID transferred from the client interface section according to a decryption algorithm **[COL.11, lines 43-57 and COL.23, lines 13-23]**, thereby extracting the first encrypted ID, and if the extracted first-encrypted ID coincides with the first encrypted ID given to the physical goods, makes request for transfer of the second execution portion of the digital goods to the client interface section

[COL.6, lines 32-40] and executes contents of the second execution portion of the digital goods transferred from the client interface section in response to the request for transfer, and wherein when the contents of the second execution portion of the digital goods are executed in the physical goods, the client interface section executes the first execution portion of the digital goods in synchronization with the execution of the contents of the second execution portion **[COL.9, lines 32-36 and COL.23, lines 13-23]**.

Wasalewski fails to explicitly discuss the registering process to show a genuine proprietor of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 13

discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 12, wherein both the

inherent ID and the first encrypted ID are incorporated into the physical goods during manufacture of the physical goods. **[COL.10, lines 27-28]**

As per claim 14

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 12, wherein the first encrypted ID given to the physical goods can be inputted from outside of the physical goods after manufacture of the physical goods. **[COL.10, lines 32-38]**

As per claim 15

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 12, wherein the physical goods prohibits the execution of the first execution portion of the digital goods in the client interface section if the extracted first-encrypted ID does not coincide with the first encrypted ID given to the physical goods. **[COL.6, lines 6-40 and COL.11, lines 46-59]**

As per claim 16

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 12, wherein the physical goods is a storytelling device, and the second execution portion includes operation code for controlling operation of the physical goods according to contents of a story and narration for dictating the contents of the story. **[COL.5, lines 44-55]**

As per claim 17

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 12, wherein the controller simultaneously transfers to the client the second encrypted ID and the digital goods requested by the client for purchase. **[COL.4, lines 1-19]**

As per claim 18

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods by use of physical goods according to claim 16, wherein the client interface is a personal computer, and the first execution portion of the digital goods includes images and sound effects. **[COL.5, lines 44-55]**

As per claim 19

Wasilewski, et al. discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, and a first encrypted ID also given thereto and encrypted from the inherent ID according to a first encryption algorithm, comprising the steps of:

obtaining the inherent ID of the physical goods by a client; **[COL.7, lines 49-55]**

transferring the obtained inherent ID together with an assignable identification name for identifying the physical goods to a business proprietor; **[COL.4, lines 20-30]**

examining whether or not a corresponding relationship between the

assignable identification name; **[COL.6, lines 7-9]**

determining a digital goods to be purchased and transferring both a code of goods and the assignable identification name corresponding to the digital goods to the business proprietor; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

identifying the first encrypted ID corresponding to the assignable identification name transferred together with the code of goods by reference to the database of the business proprietor; **[COL.10, lines 55-58]**

encrypting the first encrypted ID according to a second encryption algorithm to generate a second encrypted ID if the first encrypted ID corresponding to the assignable identification name is identified in the identifying step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

encrypting the digital goods corresponding to the code of goods according to the second encryption algorithm; **[COL.7, lines 44-45 and COL.20, lines 39-67]**

transferring the second encrypted ID and the encrypted digital goods to a client interface section; **[COL.4, lines 6-8]**

transferring the second encrypted ID and the encrypted digital goods transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

decrypting the encrypted digital goods according to the decryption algorithm if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the encrypted ID kept in the physical goods; and executing the decrypted digital goods **[COL.10, lines 43-55 and col.23, lines 30-39]**.

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 20

Wailewski discusses a method of preventing reproduction/distribution of

digital goods by use of physical goods according to claim 19, wherein the step of obtaining the inherent ID is for the client to read the inherent ID from the physical goods by initializing the physical goods through the client interface section. **[COL.5, lines 43-55]**

As per claim 21

Wailewski discusses a method of preventing reproduction/distribution of digital goods by use of physical goods according to claim 19, wherein the step of obtaining the inherent ID is to read the inherent ID which is provided to be identifiable on the outside of the physical goods. **[COL.10, lines 32-38]**

As per claim 22

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, and a first encrypted ID also given thereto and encrypted the inherent ID according to a first encryption algorithm from, comprising the steps of:

obtaining the inherent ID of the physical goods by a client; **[COL.7, lines 49-55]**

transferring the obtained inherent ID together with an assignable identification name for identifying the physical goods to a business proprietor; **[COL.4, lines 20-30]**

examining whether or not a corresponding relationship between the assignable identification name; **[COL.6, lines 7-9]**

determining a digital goods to be purchased and transferring both a code of goods and the assignable identification name corresponding to the digital goods to the business proprietor; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

identifying the first encrypted ID corresponding to the assignable identification name transferred together with the code of goods by reference to the database of the business proprietor; **[COL.10, lines 55-58]**

encrypting the first encrypted ID according to a second encryption algorithm to generate a second encrypted ID if the first encrypted ID corresponding to the assignable identification name is identified in the identifying step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

encrypting the digital goods corresponding to the code of goods according to the second encryption algorithm; **[COL.7, lines 44-45 and COL.20, lines 39-67]**

transferring the second encrypted ID and the encrypted digital goods to a client interface section; **[COL.4, lines 3-5 and COL.7, lines 44-45]**

transferring the second encrypted ID and the encrypted digital goods transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID and the encrypted digital goods transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and**

COL.23, lines 13-23]

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

executing the decrypted digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 23

Wailewski discusses a method of preventing reproduction/distribution of

digital goods by use of physical goods according to claim 22, wherein the step of obtaining the inherent ID is for the client to read the inherent ID from the physical goods by initializing the physical goods through the client interface section. **[COL.5, lines 43-55]**

As per claim 24

Wailewski discusses a method of preventing reproduction/distribution of digital goods by use of physical goods according to claim 22, wherein the step of obtaining the inherent ID is to read the inherent ID which is provided to be identifiable on the outside of the physical goods. **[COL.10, lines 32-38]**

As per claim 25

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, and a first encrypted ID also given thereto and encrypted from the inherent ID according to a first encryption algorithm, comprising the steps of:

obtaining the inherent ID of the physical goods by a client; **[COL.7, lines 49-55]**

transferring the obtained inherent ID together with an assignable identification name for identifying the physical goods to a business proprietor; **[COL.4, lines 20-30]**

determining a digital goods to be purchased which comprises a first execution portion and a second execution portion, and transferring both a code

of goods and the assignable identification name corresponding to the digital goods to the business proprietor; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

identifying the first encrypted ID corresponding to the assignable identification name transferred together with the code of goods by reference to the database of the business proprietor; **[COL.10, lines 55-58]**

encrypting the first encrypted ID according to a second encryption algorithm to generate a second encrypted ID if the first encrypted ID corresponding to the assignable identification name is identified in the identifying step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods corresponding to the code of goods to a client interface section; **[COL.4, lines 6-8]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion; **[COL.10, lines 1-8]**

transferring the second encrypted ID transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the client interface section to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.12, lines 17-50 and COL.21, lines 47-65]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section in response to the request for transfer of the digital goods and simultaneously executing contents of the first execution portion of the digital goods in the client interface section. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57

- COL.15, line 20).

As per claim 26

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, and a first encrypted ID also given thereto and encrypted from the inherent ID according to a first encryption algorithm, comprising the steps of:

obtaining the inherent ID of the physical goods by a client; **[COL.7, lines 49-55]**

transferring the obtained inherent ID together with an assignable identification name for identifying the physical goods to a business proprietor; **[COL.4, lines 20-30]**

determining a digital goods to be purchased which comprises a first execution portion and a second execution portion, and transferring both a code of goods and the assignable identification name corresponding to the digital goods to the business proprietor; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

identifying the first encrypted ID corresponding to the assignable identification name transferred together with the code of goods by reference to the database of the business proprietor; **[COL.10, lines 55-58]**

encrypting the first encrypted ID according to a second encryption algorithm to generate a second encrypted ID if the first encrypted ID corresponding to the assignable identification name is identified in the

identifying step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods corresponding to the code of goods to a client interface section; **[COL.4, lines 6-8]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion; **[COL.10, lines 1-8]**

transferring the separated second execution portion of the digital goods and the second encrypted ID transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section and simultaneously executing contents of the first execution portion of the digital goods in the client interface section, if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 27

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, and a first encrypted ID also given thereto and encrypted from the inherent ID according to a first encryption algorithm comprising the steps of:

obtaining the inherent ID of the physical goods on the side of a client; **[COL.7, lines 49-55]**

transferring the obtained inherent ID together with an assignable identification name for identifying the physical goods to a business proprietor;

[COL.4, lines 20-30]

determining a digital goods to be purchased which comprises a first execution portion and a second execution portion, and transferring both a code of goods and the assignable identification name corresponding to the digital goods to the business proprietor; **[COL.2, lines 44-48 and COL.6, lines 37-40]**

identifying the first encrypted ID corresponding to the assignable identification name transferred together with the code of goods by reference to the database of the business proprietor; **[COL.10, lines 55-58]**

encrypting the first encrypted ID according to a second encryption algorithm to generate a second encrypted ID if the first encrypted ID corresponding to the assignable identification name is identified in the identifying step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods corresponding to the code of goods to a client interface section; **[COL.4, lines 6-8]**

transferring the second encrypted ID transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the client interface section to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; **[COL.12, lines 17-50 and COL.21, lines 47-65]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion in response to the request for transfer of the digital goods; **[COL.10, lines 1-8 and COL.22, lines 31-39]**

transferring the separated second execution portion of the digital to the physical goods; and **[COL.4, lines 6-8 and COL.22, lines 56-64]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section in response to the request for transfer of the digital goods and simultaneously executing contents of the first execution portion of the digital goods in the client interface section. **[COL.23, lines 31-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of

ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 28

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, a first encrypted ID also given thereto and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods and the digital goods is sold via online from a business proprietor to a client, the method comprising the steps of:

transferring information on the physical goods including at least the assignable identification name of the physical goods and information on the digital goods including at least code of goods corresponding to the digital goods to be purchased, from the client to the business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

examining whether or not the client is a genuine proprietor of the physical goods by reference to the database of the business proprietor based on the information on the physical goods; **[COL.6, lines 7-9]**

encrypting the first encrypted ID corresponding to the identification name transferred to the business proprietor according to a second encryption algorithm, thereby generating a second encrypted ID if the genuine proprietor of the physical goods is confirmed in the examining step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

encrypting the digital goods indicated by the information on the digital goods according to the second encryption algorithm; **[COL.20, lines 59-66]**

transferring the second encrypted ID and the encrypted digital goods to a client interface section; **[COL.4, lines 6-8]**

transferring the second encrypted ID and the encrypted digital goods transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

decrypting the encrypted digital goods according to the decryption algorithm if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.22, lines 65-67]**

operating the physical goods according to contents of the decrypted

digital goods. **[COL.23, lines 31-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 29

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, a first encrypted ID also given thereto and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods and the digital goods is sold via online from a business proprietor to a client, the method comprising the steps of:

transferring information on the physical goods including at least the

assignable identification name of the physical goods and information on the digital goods including at least code of goods corresponding to the digital goods to be purchased, from the client to the business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

examining whether or not the client is a genuine proprietor of the physical goods by reference to the database of the business proprietor based on the information on the physical goods; **[COL.6, lines 7-9]**

encrypting the first encrypted ID corresponding to the identification name transferred to the business proprietor according to a second encryption algorithm, thereby generating a second encrypted ID if the genuine proprietor of the physical goods is confirmed in the examining step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

encrypting the digital goods indicated by the information on the digital goods according to the second encryption algorithm; **[COL.4, lines 3-5 and COL.7, lines 44-45]**

transferring the second encrypted ID and the encrypted digital goods to a client interface section; **[COL.4, lines 6-8]**

transferring the second encrypted ID and the encrypted digital goods transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID and the encrypted digital goods transferred to the physical goods according to a decryption algorithm

corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

operating the physical goods according to contents of the decrypted digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 30

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, a first encrypted ID also given thereto and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, and the digital goods comprises a first execution portion and a second execution portion and is sold via online from a business proprietor to a client, the method comprising the steps of:

transferring information on the physical goods including at least the assignable identification name of the physical goods and information on the digital goods including at least code of goods corresponding to the digital goods to be purchased, from the client to the business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

examining whether or not the client is a genuine proprietor of the physical goods by reference to the database of the business proprietor based on the information on the physical goods; **[COL.6, lines 7-9]**

encrypting the first encrypted ID corresponding to the assignable identification name transferred to the business proprietor according to a second encryption algorithm, thereby generating a second encrypted ID if the genuine proprietor of the physical goods is confirmed in the examining step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods indicated by the information on the digital goods to a client interface section; **[COL.4, lines 6-8]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion; **[COL.10, lines 1-8]**

transferring the second encrypted ID transferred to the client interface section to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the client interface section to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.12, lines 17-50 and COL.21, lines 47-65]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section in response to the request for transfer of the digital goods and

simultaneously executing contents of the first execution portion of the digital goods in the client interface section. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 31

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, a first encrypted ID also given thereto and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, and the digital goods comprises a first execution portion and a second execution portion and is sold

via online from a business proprietor to a client, the method comprising the steps of:

transferring information on the physical goods including at least the assignable identification name of the physical goods and information on the digital goods including at least code of goods corresponding to the digital goods to be purchased, from the client to the business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

examining whether or not the client is a genuine proprietor of the physical goods by reference to the database of the business proprietor based on the information on the physical goods; **[COL.6, lines 7-9]**

encrypting the first encrypted ID corresponding to the assignable identification name transferred to the business proprietor according to a second encryption algorithm, thereby generating a second encrypted ID if the genuine proprietor of the physical goods is confirmed in the examining step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods indicated by the information on the digital goods to a client interface section; **[COL.4, lines 6-8]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion; **[COL.10, lines 1-8]**

transferring the separated second execution portion of the digital goods

and the second encrypted ID to the physical goods; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section and simultaneously executing contents of the first execution portion of the digital goods in the client interface section, if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical

goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 32

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods wherein the physical goods has an inherent ID given thereto, a first encrypted ID also given thereto and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, and the digital goods comprises a first execution portion and a second execution portion and is sold via online from a business proprietor to a client, the method comprising the steps of:

transferring information on the physical goods including at least the assignable identification name of the physical goods and information on the digital goods including at least code of goods corresponding to the digital goods to be purchased, from the client to the business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

examining whether or not the client is a genuine proprietor of the physical goods by reference to the database of the business proprietor based on the information on the physical goods; **[COL.6, lines 7-9]**

encrypting the first encrypted ID corresponding to the assignable

identification name transferred to the business proprietor according to a second encryption algorithm, thereby generating a second encrypted ID if the genuine proprietor of the physical goods is confirmed in the examining step; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods indicated by the information on the digital goods to a client interface section; transferring the second encrypted ID to the physical goods; **[COL.4, lines 6-8]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the client interface section to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; **[COL.12, lines 17-50 and COL.21, lines 47-65]**

separating the digital goods transferred to the client interface section into the first execution portion and the second execution portion in response to the request for transfer of the digital goods; **[COL.10, lines 1-8]**

transferring the separated second execution portion of the digital to the physical goods; and **[COL.22, lines 56-64]**

executing the physical goods according to contents of the second execution portion of the digital goods transferred from the client interface section and simultaneously executing contents of the first execution portion of the digital goods in the client interface section. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 33

Wailewski discloses method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift wherein the digital goods is executed in physical goods, wherein the physical goods has an inherent ID

given thereto, ID information including a first encrypted ID which is also given to the physical goods and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, and wherein the digital goods is sold via online to a client, the method comprising the steps of:

transferring information on a gift sender, information on the digital goods to be purchased, and information on a gift recipient including the assignable identification name of the physical goods held by the gift recipient from the gift sender to a business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

extracting the ID information of the physical goods held by the gift recipient by reference to a database of the business proprietor; **[COL.6, lines 32-40]**

encrypting the first encrypted ID among the extracted ID information according to a second encryption algorithm, thereby generating a second encrypted ID; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

encrypting the digital goods selected by the gift sender according to the second encryption algorithm; **[COL.4, lines 3-5 and COL.7, lines 44-45]**

transferring the second encrypted ID and the encrypted digital goods to a interface section of the gift recipient; **[COL.4, lines 6-8]**

transferring the second encrypted ID and the encrypted digital goods transferred to the interface section of the gift recipient to the physical goods of the gift recipient; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

decrypting the encrypted digital goods according to the decryption algorithm if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.23, lines 13-23]**

executing contents of the decrypted digital goods provided as the gift in the physical goods.

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or

a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 34

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift according to claim 33, wherein the step of transferring the second encrypted ID and the encrypted digital goods to the interface section of the gift recipient includes the steps of:

transferring information including information that the digital goods has been provided by the gift sender, URL of the business proprietor, and guide information for downloading the gift to the interface section of the gift recipient, to an email address of the gift recipient; **[COL.12, lines 48-60]**

aproviding an access to the URL of the business proprietor by the gift recipient by confirming the email; and

downloading the digital goods provided as the gift by the gift recipient from the URL of the business proprietor to the interface section.

As per claim 35

discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift wherein the digital goods is executed in physical goods, wherein the physical goods has an inherent ID given thereto, ID information including a first encrypted ID which is also given to the physical

goods and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, and wherein the digital goods is sold via online to a client, the method comprising the steps of:

transferring information on a gift sender, information on the digital goods to be purchased, and information on a gift recipient including the assignable identification name of the physical goods held by the gift recipient from the gift sender to a business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

extracting the ID information of the physical goods held by the gift recipient by reference to a database of the business proprietor; **[COL.6, lines 32-40]**

encrypting the first encrypted ID among the extracted ID information according to a second encryption algorithm, thereby generating a second encrypted ID; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-65]**

encrypting the digital goods selected by the gift sender according to the second encryption algorithm; **[COL.4, lines 3-5 and COL.7, lines 44-45]**

transferring the second encrypted ID and the encrypted digital goods to a interface section of the gift recipient; **[COL.4, lines 6-8]**

transferring the second encrypted ID and the encrypted digital goods transferred to the interface section of the gift recipient to the physical goods of the gift recipient; **[COL.22, lines 56-64]**

decrypting the second encrypted ID and the encrypted digital goods

transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

executing contents of the decrypted digital goods provided as the gift in the physical goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted coincides with the first encrypted ID given to the physical goods.

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 36

Kupka discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift according to claim 35, wherein the step of transferring the second encrypted ID and the encrypted digital goods to the interface section of the gift recipient includes the steps of:

transferring information including information that the digital goods has been provided by the gift sender, URL of the business proprietor, and guide information for downloading the gift to the interface section of the gift recipient, to an email address of the gift recipient; **[COL.13, lines 26-41]**

providing an access to the URL of the business proprietor by the gift recipient by confirming the email; and **[COL.83, lines 40-47]**

downloading the digital goods provided as the gift by the gift recipient from the URL of the business proprietor to the interface section **[COL.7, lines 48-55]**

As per claim 37

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift wherein the digital goods sold via online to a client comprises a first execution portion and a second execution portion, wherein the second execution portion of the digital goods is executed in physical goods, and wherein the physical goods has an inherent ID given

thereto, ID information including a first encrypted ID which is also given to the physical goods and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, the method comprising the steps of:

transferring information on a gift sender, information on the digital goods to be purchased, and information on a gift recipient including the assignable identification name of the physical goods held by the gift recipient from the gift sender to a business proprietor; **[COL.4, lines 20-30 and COL.7, lines 49-55]**

extracting the ID information of the physical goods held by the gift recipient by reference to a database of the business proprietor; **[COL.6, lines 32-40]**

encrypting the first encrypted ID among the extracted ID information according to a second encryption algorithm, thereby generating a second encrypted ID; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods selected by the gift sender to a interface section of the gift recipient;

separating the digital goods into the first execution portion and the second execution portion; **[COL.10, lines 1-8]**

transferring the second encrypted ID transferred to the interface section of the gift recipient to the physical goods of the gift recipient; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods

according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the interface section of the gift recipient to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.12, lines 17-50 and COL.21, lines 47-65]**

executing contents of the second execution portion of the digital goods transferred from the interface section of the gift recipient in response to the request for transfer in the physical goods and simultaneously executing contents of the first execution portion of the digital goods in the interface section of the gift recipient. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of

Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 38

Kupka discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift according to claim 37, wherein the step of transferring the second encrypted ID and the encrypted digital goods to the interface section of the gift recipient includes the steps of:

transferring information including information that the digital goods has been provided by the gift sender, URL of the business proprietor, and guide information for downloading the gift to the interface section of the gift recipient, to an email address of the gift recipient; **[COL.13, lines 26-41]**

providing an access to the URL of the business proprietor by the gift recipient by confirming the email; and **[COL.83, lines 40-47]**

downloading the digital goods provided as the gift by the gift recipient from the URL of the business proprietor to the interface section. **[COL.7, lines 48-55]**

As per claim 39

Wailewski discloses a method of preventing reproduction/distribution of digital

goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift wherein the digital goods sold via online to a client comprises a first execution portion and a second execution portion, wherein the second execution portion of the digital goods is executed in physical goods, and wherein the physical goods has an inherent ID given thereto, ID information including a first encrypted ID which is also given to the physical goods and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, the method comprising the steps of:

transferring information on a gift sender, information on the digital goods to be purchased, and information on a gift recipient including the assignable identification name of the physical goods held by the gift recipient from the gift sender to a business proprietor;

extracting the ID information of the physical goods held by the gift recipient by reference to a database of the business proprietor; **[COL.6, lines 32-40]**

encrypting the first encrypted ID among the extracted ID information according to a second encryption algorithm, thereby generating a second encrypted ID; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods selected by the gift sender to a interface section of the gift recipient; **[COL.4, lines 6-8]**

separating the digital goods into the first execution portion and the

second execution portion; **[COL.10, lines 1-8]**

transferring the separated second execution portion and the second encrypted ID transferred to the interface section of the gift recipient to the physical goods of the gift recipient; **[COL.22, lines 56-64]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; and **[COL.11, lines 55-59 and COL.22, lines 56-65]**

executing contents of the second execution portion of the digital goods in the physical goods and simultaneously executing contents of the first execution portion of the digital goods in the interface section of the gift recipient, if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of

ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 40

Kupka discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift according to claim 39 wherein the step of transferring the second encrypted ID and the encrypted digital goods to the interface section of the gift recipient includes the steps of:

transferring information including information that the digital goods has been provided by the gift sender, URL of the business proprietor, and guide information for downloading the gift to the interface section of the gift recipient, to an email address of the gift recipient; **[COL.13, lines 26-41]**

providing an access to the URL of the business proprietor by the gift recipient by confirming the email; and **[COL.83, lines 40-47]**

downloading the digital goods provided as the gift by the gift recipient from the URL of the business proprietor to the interface section. **[COL.7, lines 48-55]**

As per claim 41

Wailewski discloses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift wherein the digital goods sold via online to a client comprises a first execution portion and a second execution portion, wherein the second execution portion of the digital goods is executed in physical goods, and wherein the physical goods has an inherent ID given thereto, ID information including a first encrypted ID which is also given to the physical goods and encrypted from said inherent ID according to a first encryption algorithm and an assignable identification name for identifying the physical goods, the method comprising the steps of:

transferring information on a gift sender, information on the digital goods to be purchased, and information on a gift recipient including the assignable identification name of the physical goods held by the gift recipient from the gift sender to a business proprietor;

extracting the ID information of the physical goods held by the gift recipient by reference to a database of the business proprietor; **[COL.6, lines 32-40]**

encrypting the first encrypted ID among the extracted ID information according to a second encryption algorithm, thereby generating a second encrypted ID; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

transferring the second encrypted ID and the digital goods selected by

the gift sender to a interface section of the gift recipient; transferring the second encrypted ID transferred to the interface section of the gift recipient to the physical goods of the gift recipient; **[COL.4, lines 6-8]**

decrypting the second encrypted ID transferred to the physical goods according to a decryption algorithm corresponding to the second encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

comparing the first encrypted ID generated by the decryption of the second encrypted ID with the first encrypted ID given to the physical goods; **[COL.11, lines 55-59 and COL.22, lines 56-65]**

requesting the interface section of the gift recipient to transfer the second execution portion of the digital goods if, in the comparing step, the first encrypted ID generated by the decryption of the second encrypted ID coincides with the first encrypted ID given to the physical goods; **[COL.12, lines 17-50 and COL.21, lines 47-65]**

separating the digital goods transferred to the interface section of the gift recipient into the first execution portion and the second execution portion in response to the request for transfer of the second execution portion of the digital goods; **[COL.10, lines 1-8]**

transferring the separated second execution portion of the digital to the physical goods; and **[COL.22, lines 56-64]**

executing contents of the second execution portion of the digital goods transferred to the physical goods in the physical goods and simultaneously

executing contents of the first execution portion of the digital goods in the interface section of the gift recipient. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 42

Kupka discusses a method of preventing reproduction/distribution of digital goods by use of physical goods so as to permit sending a gift of the digital goods to a third party and receiving the gift according to claim 41, wherein the step of transferring the second encrypted ID and the encrypted digital goods to the interface section of the gift recipient includes the steps of:

transferring information including information that the digital goods has

been provided by the gift sender, URL of the business proprietor, and guide information for downloading the gift to the interface section of the gift recipient, to an email address of the gift recipient; **[COL.13, lines 26-41]**

providing an access to the URL of the business proprietor by the gift recipient by confirming the email; and **[COL.83, lines 40-47]**

downloading the digital goods provided as the gift by the gift recipient from the URL of the business proprietor to the interface section. **[COL.7, lines 48-55]**

As per claim 43

discloses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device, comprising:

the operation device for executing a part of the digital contents the operation device including an inherent ID given thereto, a first encrypted ID also given thereto and encrypted according to a first encryption algorithm from said inherent ID, and an assignable identification name for identifying the operation device; **[COL.12, lines 53-57]**

providing an authentication code including a second encrypted ID generated by encrypting the first encrypted ID stored in the database of the central controller according to a second encryption algorithm when the authentication code is requested; **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**

an electronic commerce controller for requesting the authentication code

to the central controller based on the digital contents information and the purchase information including the assignable identification name, generating a signal for requesting the digital contents selected by the client if the authentication code is provided from the central controller, and providing the digital contents and the authentication code to be provided according to the requests with the client interface section; and **[COL.12, lines 17-50 and COL.21, lines 47-65]**

a digital contents controller for providing the requested digital contents with the electronic commerce controller when the signal for requesting the digital contents is received, wherein the client interface section transfers the part of the digital contents and the authentication code to the operation device when the purchased digital contents and the authentication code are received **[COL.6, lines 1-40 and COL.20, lines 57-67]**, wherein the operation device decrypts the second encrypted ID included in authentication code according to a decryption algorithm corresponding to the second encryption algorithm to extract the first encrypted ID when the part of the digital contents and the authentication code are received **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-65]** and executes the part of the digital contents transferred from the client interface section only when the extracted first-encrypted ID coincides with the first encrypted ID given to the operation device **[COL.6, lines 32-40]**, and wherein the client interface section executes the remaining part of the digital contents except the part which has been transferred to the operation

device and is executed by the operation device, in synchronization with the execution of the part on the side of the operation device. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 44

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 43, wherein the client interface section reads the inherent ID from the operation device by an operation device set-up program. **[COL.20, lines 57-67]**

As per claim 45

discusses a system of preventing reproduction/distribution of digital contents

sold via online by use of an operation device according to claim 43, wherein the client interface section provides the inherent ID identified from outside of the operation device. **[COL.12, lines 53-57]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 46

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 43, wherein the central controller, the electronic commerce controller, and the digital contents controller are managed by a business proprietor. **[COL.6, lines 1-40 and COL.20, lines 57-67]**

As per claim 47

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 43, wherein the central controller, the electronic commerce controller, and the digital contents controller are separately managed. **[COL.6, lines 1-40 and COL.20, lines 57-67]**

As per claim 48

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 43, wherein a business proprietor who manages the central controller and the electronic commerce controller is different from a business proprietor who manages the digital contents controller. **[COL.6, lines 1-40 and COL.20, lines 57-67]**

As per claim 49

Wailewski discloses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device, comprising:

the operation device for executing a part of the digital contents, the operation device including an inherent ID given thereto, a first encrypted ID also given thereto and encrypted according to a first encryption algorithm from said inherent ID, and an assignable identification name for identifying the operation device; **[COL.7, lines 44-45 and COL.20, lines 39-67]**

a client interface section for providing information on digital contents to be purchased and purchase information including the assignable identification

name to purchase the digital contents; **[COL.6, lines 1-40 and COL.20, lines 57-67]**

providing an authentication code including a second encrypted ID generated by encrypting the first encrypted ID stored in the database of the central controller according to a second encryption algorithm when the authentication code is requested; **[COL.9, lines 14-65]**

an electronic commerce controller for requesting the authentication code to the central controller based on the digital contents information and the purchase information including the assignable identification name, generating a signal for requesting the digital contents selected by the client if the authentication code is provided from the central controller, and providing the digital contents and the authentication code to be provided according to the requests with the client interface section; and **[COL.12, lines 17-50 and COL.21, lines 47-65]**

a digital contents controller for providing the requested digital contents with the electronic commerce controller when the signal for requesting the digital contents is received, wherein the client interface section transfers the authentication code to the operation device when the purchased digital contents and the authentication code are received, wherein the operation device decrypts the second encrypted ID included in authentication code according to a decryption algorithm **[COL.11, lines 43-57 and COL.23, lines 13-23]** corresponding to the second encryption algorithm to extract the first

encrypted ID when the authentication code is received, receives the part of the digital contents from the client interface section only when the extracted first-encrypted ID **[COL.6, lines 32-40]** coincides with the first encrypted ID given to the operation device, and executes the part of the digital contents **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-65]**, and wherein the client interface section executes the remaining part of the digital contents except the part which has been transferred to the operation device, in synchronization with the execution of the part on the side of the operation device. **[COL.10, lines 43-55 and col.23, lines 30-39]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 50

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 49, wherein the client interface section reads the inherent ID from the operation device by an operation device set-up program. **[COL.12, lines 53-57]**

As per claim 51

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 49, wherein the client interface section provides the inherent ID identified from outside of the operation device. **[COL.12, lines 53-57]**

Wasalewski fails to explicitly discuss the registering process of the physical goods.

Kupka discloses the registering process to show a genuine proprietor of the physical goods (removable media) that uses an inherently unique serial number, key, name, vendor ID, etc. to register the media (COL.12, lines 48-52). It would have been obvious for one of ordinary skill in the art to combine Kupka with the teachings of Wasilewski to register so as to show the genuine proprietor of the physical goods because of the added security and safeguards to promote additional layers of security to prevent unauthorized decryption of protected data or a program that was not approved by a provider or vendor (COL.14, line 57 - COL.15, line 20).

As per claim 52

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 49, wherein the central controller, the electronic commerce controller, and the digital contents controller are managed by a business proprietor. **[COL.6, lines 1-40 and COL.20, lines 57-67]**

As per claim 53

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 49, wherein the central controller, the electronic commerce controller, and the digital contents controller are separately managed. **[COL.6, lines 1-40 and COL.20, lines 57-67]**

As per claim 54

Wailewski discusses a system of preventing reproduction/distribution of digital contents sold via online by use of an operation device according to claim 49, wherein a business proprietor who manages the central controller and the electronic commerce controller is different from a business proprietor who manages the digital contents controller. **[COL.5, lines 40-47 and COL.6, lines 1-40]**

As per claim 55

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods sold via online to a client by use of physical goods having an

inherent ID and a first encrypted ID from said inherent ID encrypted according to a first encryption algorithm for executing a part of the sold digital goods **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, wherein the physical goods comprises a controller for determining the execution of the part of the sold digital goods depending on a result of comparison of a decrypted ID generated by decrypting a second encrypted ID **[COL.11, lines 43-57 and COL.23, lines 13-23]**, which had been generated by encrypting the first encrypted ID according to a second encryption algorithm and transferred to the physical goods when selling the digital goods, with the first encrypted ID given to the physical goods. **[COL.11, lines 55-59 and COL.22, lines 56-65]**

As per claim 56

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods sold via online to a client by use of physical goods having a first encrypted ID for executing a part of the sold digital goods **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, wherein the physical goods comprises a controller for determining the execution of the part of the sold digital goods depending on a result of comparison of a decrypted ID generated by decrypting a second encrypted ID **[COL.11, lines 43-57 and COL.23, lines 13-23]**, which had been generated by encrypting the first encrypted ID according to an encryption algorithm and transferred to the physical goods when selling the digital goods, according to a decryption algorithm corresponding to the encryption algorithm with the first encrypted ID given to the physical goods.

[COL.11, lines 55-59 and COL.22, lines 56-65]

As per claim 57

Wailewski discusses a method of preventing reproduction/distribution of digital goods transferred via online by use of physical goods having a first encrypted ID given thereto for executing a part of the transferred digital goods, comprising the steps of:

requesting transfer of the digital goods to a proprietor of the physical goods by purchasing of the digital goods; **[COL.12, lines 17-50 and COL.21, lines 47-65]**

examining whether or not the proprietor of the physical goods is a genuine one; **[COL.6, lines 7-9]**

transferring the digital goods and a second encrypted ID generated by encrypting the first encrypted ID according to a predetermined encryption algorithm to the proprietor of the physical goods; **[COL.4, lines 3-5 and COL.7, lines 44-45]**

decrypting the second encrypted ID transferred to the proprietor of the physical goods according to a decryption algorithm corresponding to the predetermined encryption algorithm; and **[COL.11, lines 43-57 and COL.23, lines 13-23]**

determining the execution of the part of the transferred digital goods depending on a result of comparison of the decrypted ID with the first encrypted ID given to the physical goods. **[COL.11, lines 55-59 and COL.22,**

lines 56-65]

As per claim 58

Wailewski discloses a method of preventing reproduction/distribution of digital goods comprising a first execution portion and a second execution portion transferred via online by use of physical goods having a first encrypted ID given thereto for executing the second execution portion of the digital goods, comprising the steps of:

requesting transfer of the digital goods to a proprietor of the physical goods by purchasing of the digital goods; **[COL.12, lines 17-50 and COL.21, lines 47-65]**

examining whether or not of the physical goods is a genuine one; **[COL.6, lines 7-9]**

transferring the digital goods and a second encrypted ID generated by encrypting the first encrypted ID according to a predetermined encryption algorithm to the proprietor of the physical goods; **[COL.7, lines 44-45 and COL.20, lines 39-67]**

decrypting the second encrypted ID transferred to the proprietor of the physical goods according to a decryption algorithm corresponding to the predetermined encryption algorithm; **[COL.11, lines 43-57 and COL.23, lines 13-23]**

determining whether or not the decrypted ID coincides with the first encrypted ID given to the physical goods; and **[COL.2, lines 44-48 and COL.6,**

lines 37-40]

executing the second execution portion of the digital goods in the physical goods and simultaneously executing the first execution portion of the digital goods in an interface section of the proprietor connected to the physical goods in synchronization with the execution of the second execution portion only when, in the determining step, the decrypted ID coincides with the first encrypted ID given to the physical goods. **[COL.10, lines 43-55 and col.23, lines 30-39]**

As per claim 59

Wailewski discusses an apparatus for preventing reproduction/distribution of digital goods transferred via online by use of physical goods having a first encrypted ID given thereto for executing a part of the transferred digital goods **[COL.3, line 67 – COL.4, line 1 and COL.9, lines 14-15]**, wherein the physical goods determines the execution of the part of the transferred digital goods depending on a result of comparison of a decrypted ID generated by decrypting a second encrypted ID **[COL.11, lines 43-57 and COL.23, lines 13-23]**, which had been generated by encrypting the first encrypted ID according to a predetermined encryption algorithm and transferred to the physical goods, according to a decryption algorithm corresponding to the predetermined encryption algorithm, with the first encrypted ID given to the physical goods. **[COL.11, lines 55-59 and COL.22, lines 56-65]**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

LHa